DETAILED ACTION

1. This office action is in response to Applicant's amendment filed on July 21, 2010.

2. Claims 1, 8, 10-11, 13-15 and 17 have been amended.

3. Claims 7, 9 and 16 have been cancelled.

4. New claims 21-24 have been added.

5. Claims 1-6, 8, 10-15 and 17-24 are pending.

EXAMINER'S AMENDMENT

6. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

7. Authorization for this examiner's amendment was given in a telephone interview with Kien Le (Reg. No. 64,167) on 09/22/10.

The application has been amended as follows:

Please amend the claims as follows:

Please cancel claims 21 and 23.

Claim 1:

An apparatus connected [to be connected] between a network access unit and a network to be protected, for protecting legitimate traffic from DoS (denial of service) and DDoS (distributed denial of service) attacks, said apparatus comprising:

a hardware unit which is connected between the network access unit and the network to be protected;

said hardware unit comprising:

a high-priority queue;

a low-priority queue;

a queue information table having, for each specific STT (source-based traffic trunk),

previous load information, and

a service queue for a specific packet having the specific STT, wherein the service queue is the high-priority queue or the low-priority queue;

a packet classifier for

(a) obtaining an STT of a packet received from the network access unit based on a source IP address of the received packet ;

(b) searching the queue information table for the service queue corresponding to the STT of the received packet and checking, by the packet classifier, whether the service queue is the high-priority queue or the low-priority queue;

(c) transferring the received packet to the high-priority queue if the service queue is the high-priority queue in the step (b);

(d) transferring the received packet to the low-priority queue if the service queue is the low-priority queue in the step (b); and

(e) transferring packet information on the received packet to a queue coordinator;

said queue coordinator for

(f) updating the service queue associated with the STT of the received packet in the queue information table, wherein said updating is based on (i) a load of the received packet and (ii) the previous load information stored in the queue information table in association with the STT of the received packet;

wherein said updating at (f) comprises:

(a') calculating an average load of the STT of the received packet based on the packet information transferred from the packet classifier;

(b') selectively resetting the service queue associated with the STT of the received packet depending on the calculated average load of the STT of the received packet; and

(c') storing the selectively reset service queue in the queue information table; and

wherein said selectively resetting at (b') further includes:

(b'1) setting the service queue associated with the STT of the received packet to be the low-priority queue if the calculated average load of the STT of the received packet is greater than an allowable load when the high-priority queue is in a congested state;

(b'2) randomly choosing a first STT, which uses the low-priority queue, from the queue information table if the service queue associated with the STT of the received packet is the high-priority queue;

(b'3) following the step (b'2), setting a service queue associated with the randomly chosen first STT to be the high-priority queue and the service queue associated with the STT of the received packet to be the low-priority queue if the average load of the STT of the received packet is greater than that of the randomly chosen first STT;

(b'4) randomly choosing a second STT, which uses the high-priority queue, from the queue information table if the service queue associated with the STT of the received packet is the low-priority queue; and

(b'5) following the step (b'4), setting the service queue associated with the STT of the received packet to be the high-priority queue and a service queue associated with the randomly chosen second STT to be the low-priority queue if the average load of the STT of the received packet is smaller than that of the randomly chosen second STT; and

a buffer for buffering outputs of the high-priority queue and the low-priority queue and providing the buffered outputs to the network to be protected.

Claim 13:

A method of protecting legitimate traffic from DoS (denial of service) and DDoS (distributed denial of service) attacks, said method [being] performed by an apparatus

which is a hardware unit connected between a network access unit and a network to be protected and [which includes] including:

a queue information table having, for each specific STT (source-based traffic trunk),

previous load information, and

a service queue for a specific packet having the specific STT, wherein the service queue is a high-priority queue or a low-priority queue,

a queue coordinator, and

a packet classifier,

the method comprising the steps of:

(a) obtaining, by the packet classifier in said hardware unit, an STT of a packet received from the network access unit based on a source IP address of the received packet ;

(b) searching, by the packet classifier, the queue information table for the service queue corresponding to the STT of the received packet and checking, by the packet classifier, whether the service queue is the high-priority queue or the low-priority queue;

(c) transferring, by the packet classifier, the received packet to the high-priority queue if the service queue is the high-priority queue in the step (b);

(d) transferring, by the packet classifier, the received packet to the low-priority queue if the service queue is the low-priority queue in the step (b);

(e) transferring, by the packet classifier, packet information on the received packet to the queue coordinator; and

(f) updating, by the queue coordinator in said hardware unit, the service queue associated with the STT of the received packet in the queue information table, wherein said updating is based on (i) a load of the received packet and (ii) the previous load information stored in the queue information table in association with the STT of the received packet;

wherein the step (f) comprises the following steps performed by the queue coordinator:

(a') calculating an average load of the STT of the received packet based on the packet information transferred from the packet classifier;

(b') selectively resetting the service queue associated with the STT of the received packet depending on the calculated average load of the STT of the received packet;

(c') calculating an average load of the high-priority queue;

(d') selectively resetting a service queue associated with a certain STT depending on the calculated average load of the high-priority queue; and

(e') storing the selectively reset service queue in the queue information table; and

wherein the step (b') further includes the steps of:

(b'1) setting the service queue associated with the STT of the received packet to be the low-priority queue if the calculated average load of the STT of the received packet is greater than an allowable load when the high-priority queue is in a congested state;

(b'2) randomly choosing a first STT, which uses the low-priority queue, from the queue information table if the service queue associated with the STT of the received packet is the high-priority queue;

(b'3) following the step (b'2), setting a service queue in said hardware unit associated with the randomly chosen first STT to be the high-priority queue and the service queue associated with the STT of the received packet to be the low-priority queue if the average load of the STT of the received packet is greater than that of the randomly chosen first STT;

(b'4) randomly choosing a second STT, which uses the high-priority queue, from the queue information table if the service queue associated with the STT of the received packet is the low-priority queue; and

(b'5) following the step (b'4), setting the service queue associated with the STT of the received packet to be the high-priority queue and a service queue associated with the randomly chosen second STT to be the low-priority queue if the average load of the STT of the received packet is smaller than that of the randomly chosen second STT.

Claim 15:

A method of protecting legitimate traffic from DoS (denial of service) and DDoS (distributed denial of service) attacks, said method ~~being~~ performed by an apparatus which is a hardware unit connected between a network access unit and a network to be protected and including [includes]:

a queue information table having, for each specific STT (source-based traffic trunk),

previous load information, and

a service queue for a specific packet having the specific STT,

wherein the service queue is a high-priority queue or a low-priority queue,

a queue coordinator, and

a packet classifier,

the method comprising the steps of:

(a) obtaining, by the packet classifier in said hardware unit, an STT of a packet received from the network access unit based on a source IP address of the received packet ;

(b) searching, by the packet classifier, the queue information table for the service queue corresponding to the STT of the received packet and checking, by the packet classifier, whether the service queue is the high-priority queue or the low-priority queue;

(c) transferring, by the packet classifier, the received packet to the high-priority queue if the service queue is the high-priority queue in the step (b);

(d) transferring, by the packet classifier, the received packet to the low-priority queue if the service queue is the low-priority queue in the step (b);

(e) transferring, by the packet classifier, packet information on the received packet to the queue coordinator; and

(f) updating, by the queue coordinator in said hardware unit, the service queue associated with the STT of the received packet in the queue information table, wherein said updating is based on (i) a load of the received packet and (ii) the previous load information stored in the queue information table in association with the STT of the received packet;

wherein the step (f) comprises the following steps performed by the queue coordinator :

(a') calculating an average load of the STT of the received packet based on the packet information transferred from the packet classifier;

(b') selectively resetting the service queue associated with the STT of the received packet depending on the calculated average load of the STT of the received packet;

(c') calculating an average load of the high-priority queue;

(d') selectively resetting a service queue associated with a certain STT depending on the calculated average load of the high-priority queue; and

(e') storing the selectively reset service queue in the queue information table; and

wherein the step (d') includes the steps of:

(d'1) obtaining the calculated average load of the high-priority queue from the step (c');

(d'2) randomly choosing one STT, which uses the high-priority queue, and setting a service queue of the randomly chosen STT to the low-priority queue if the calculated average load of the high-priority queue indicates that the high-priority queue is in a congested state;

(d'3) randomly choosing one STT, which uses the low-priority queue, and setting a service queue of the randomly chosen STT to the high-priority queue if the calculated average load of the high-priority queue indicates that the high-priority queue is in an idle state; and

(d'4) proceeding to the step (e') if the calculated average load of the high-priority queue indicates that the high-priority queue is in a stable state or when one of the steps of (d'2) and (d'3) is performed.

Claim 17:

A method of protecting legitimate traffic from DoS (denial of service) and DDoS (distributed denial of service) attacks, said method ~~being~~ performed by an apparatus which is a hardware unit connected between a network access unit and a network to be protected and including [which includes]:

a queue information table having, for each specific STT (source-based traffic trunk),

previous load information, and

a service queue for a specific packet having the specific STT,

wherein the service queue is a high-priority queue or a low-priority queue,

a queue coordinator, and

a packet classifier,

the method comprising the steps of:

(a) obtaining, by the packet classifier in said hardware unit, an STT of a packet received from the network access unit based on a source IP address of the received packet ;

(b) searching, by the packet classifier, the queue information table for the service queue corresponding to the STT of the received packet and checking, by the packet classifier, whether the service queue is the high-priority queue or the low-priority queue;

(c) transferring, by the packet classifier, the received packet to the high-priority queue if the service queue is the high-priority queue in the step (b);

(d) transferring, by the packet classifier, the received packet to the low-priority queue if the service queue is the low-priority queue in the step (b);

(e) transferring, by the packet classifier, packet information on the received packet to the queue coordinator; and

(f) updating, by the queue coordinator in said hardware unit, the service queue associated with the STT of the received packet in the queue information table, wherein said updating is based on (i) a load of the received packet and (ii) the previous load information stored in the queue information table in association with the STT of the received packet;

wherein the step (f) comprises the following steps performed by the queue coordinator:

(a') calculating an average load of the STT of the received packet based on the packet information transferred from the packet classifier;

(b') selectively resetting the service queue associated with the STT of the received packet depending on the calculated average load of the STT of the received packet; and

(c') storing the selectively reset service queue in the queue information table; and

wherein the step (b') further includes the steps of:

(b'1) setting the service queue associated with the STT of the received packet to be the low-priority queue if the calculated average load of the STT of the received packet is greater than an allowable load when the high-priority queue is in a congested state;

(b'2) randomly choosing a first STT, which uses the low-priority queue, from the queue information table if the service queue associated with the STT of the received packet is the high-priority queue;

(b'3) following the step (b'2), setting a service queue associated with the randomly chosen first STT to be the high-priority queue and the service queue associated with the STT of the received packet to be the low-priority queue if the average load of the STT of the received packet is greater than that of the randomly chosen first STT;

(b'4) randomly choosing a second STT, which uses the high-priority queue, from the queue information table if the service queue associated with the STT of the received packet is the low-priority queue; and

(b'5) following the step (b'4), setting the service queue associated with the STT of the received packet to be the high-priority queue and a service queue associated with the randomly chosen second STT to be the low-priority queue if the average load of the STT of the received packet is smaller than that of the randomly chosen second STT.

Allowable Subject Matter

8. Claims 1-6, 8, 10-15, 17-20, 22 and 24 are allowed.

The following is an examiner's statement of reasons for allowance: The prior art on record teaches:

Moran (US 7,299,277) teaches a probe apparatus for application monitoring including a flow processor coupled to a data collection module classifies the collected data into a plurality of flows. A capture system coupled to the flow processor filters and

buffers the collected data wherein the capture buffer is segmented into priority queue and non-priority queue and the buffer space for each queue varies dynamically based on the arrival of data that meets the priority criteria.

Maher (US 2003/0227942) teaches method and apparatus for preventing denial of service attack scanning the contents of the data packets flowing over the data network using a traffic flow scanning engine. The data packets are reordered and reassembled and then the payload contents are scanned to determine whether they conform to predetermined requirements The traffic flow scanning engine is further operable to determine whether the data packets are associated with validated traffic flows and validated traffic flows are assigned to a higher priority while those not associated with a validated traffic flow are assigned to a low priority.

Kargl teaches providing protecting from DoS and DDoS attacks using a traffic monitor that runs on a load balancer and all web servers. It monitors the network for packets destined to or originating from web service address. If it finds certain IP addresses are emitting or receiving too many traffic or if the packet/size ratio falls under certain amount it marks the IP address as a potential attacker.

However, the prior art on record either taken singularly or in combination fails to teach: the specific way protecting legitimate traffic from DoS and DDoS including the steps performed by the packet classifier and the queue coordinator as recited in the independent claims.

Dependent claims 2-6, 8, 10-12, 18-20, 22 and 24 are also allowed.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHEWAYE GELAGAY whose telephone number is (571)272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Shewaye Gelagay/
Examiner, Art Unit 2437

/Matthew B Smithers/
Primary Examiner, Art Unit 2437